UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/920,784	08/01/2001	Roberto Fabian Averbuj	010343	5164

23696 7590 05/13/2005

Qualcomm Incorporated
Patents Department
5775 Morehouse Drive
San Diego, CA 92121-1714

EXAMINER	
UNGAR, DANIEL M	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 05/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/920,784	AVERBUJ ET AL.	
	Examiner	Art Unit	
	Daniel M. Ungar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *01 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 August 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2/10/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED OFFICE ACTION

1. Claims 1-25 have been examined.

CLAIM REJECTIONS 35 U.S.C. 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1, 9, 10, 16, and 17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. Claims 8-14 are indefinite because it is unclear how rounds, functions, and sub-key generators, which are themselves abstract entities, can comprise memory and registers, even though an apparatus may comprise the rounds, functions, and generators, which utilize memory and registers.

5. Claim 1 recites, "the KASUMI cipher", for which there is insufficient antecedent basis.

6. Claim 9 recites, "the output of the XOR gate" for which there is insufficient antecedent basis.

7. Claim 10 recites, "the contents of the memory" for which there is insufficient antecedent basis.

8. Claim 16 recites, "the input", "the calculating step", "the stored result". There is insufficient antecedent basis for the limitations of this claim.

9. Claim 17 recites, "the FL function", "the FO function", "the partial result", "the upper half of the input", "the lower half of the input". There is insufficient antecedent basis for the limitations of this claim.

CLAIM REJECTIONS - 35 U.S.C. 101

10. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

11. Claims 1 and 2 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Although an apparatus usually implies hardware, the limitations claimed lack the requisite tangible hardware to establish statutory basis.

CLAIM REJECTIONS - 35 U.S.C. 102

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

13. Claims 1-4 and 8-25 are rejected under 35 U.S.C. 102(b) as being anticipated by the KASUMI Specification Version 1.0, 3GPP, 23 December 1999 (hereinafter "the KASUMI Specification).

14. Regarding claim 1, the KASUMI Specification discloses generating a fractional portion of the KASUMI cipher operably coupled to a calculation controller for sequencing eight rounds to produce a KASUMI output (see paragraph 3.2).

15. Regarding claims 2, 4, 14, 15, 18, and 23-25, the KASUMI Specification discloses a sub-key generator for each of eight rounds based on the 128-bit key, using shift registers, masking, and rotating (see paragraph 4.6).

16. Regarding claims 3 and 8, the KASUMI Specification discloses performing KASUMI with a key comprising generating a fractional portion of the KASUMI cipher, configurable for calculation of even and odd rounds for eight rounds (see paragraph 4.1), storing the output of the KASUMI round and providing input to the KASUMI round, the input being selected during the first round and the contents of the memory being selected during subsequent rounds (see paragraph 4.1; page 24, function Kasumi), and each round receiving an input and producing an output, operable with a partial round calculator, storing an intermediate value from the partial round calculator, and selecting between the input and the contents of the memory for delivery to the partial round calculator (see paragraph 4.1; page 24, function Kasumi).

17. Regarding claim 9, the KASUMI Specification discloses

A KASUMI round for receiving a 64-bit input and producing a 64-bit output comprising:

an FO function, an FL function, an XOR gate, a first register,

a second register for receiving the outputg of the XOR gate, the output being concatenated with the output of the first register to produce the 64-bit output;

a first input mux for selecting between the upper half of the 64-bit input and the output of the second register under control of an input select signal, the output being received at the first register;

a second input mux for selecting between the lower half of the 64-bit input and the output of the first register under control of the input select signal, the output being delivered as the second operand to the XOR gate;

a first datapath mux, the output of which is delivered to the FL function, for selecting between the output of the first input mux and the output of the FO function under control of a data flow signal;

a second datapath mux, the output of which is delivered to the FO function, for selecting between the output of the FL function and the output of the first register under control of the data flow signal; and

a third datapath mux, the output of which is delivered as the first operand to the XOR gate, for selecting between the output of the FL function and the FO function under control of the data flow signal (see paragraphs 4.1-4.4).

18. Regarding claims 10, 11, 19, and 20, the KASUMI Specification discloses an FO function which receives an input, produces an output, uses XOR gates, calculates partial results and stores intermediate values, and selects between the input and the stored result (see paragraph 4.3; page 23, function FO).

19. Regarding claims 12, 13, 21, and 22, the KASUMI Specification discloses an FI function which receives an input, produces an output, uses XOR gates, muxes, and S9 and S7 functions, calculates partial results and stores intermediate values, and selects between the input and the stored result (see paragraph 4.4, page 22, function FI).

20. Regarding claim 16, the KASUMI Specification discloses eight rounds of KASUMI ciphering, calculating step in which the input is selected during the first round and the stored result is selected during subsequent rounds, calculating and storing a partial result, and delivering the stored result as output (see paragraph 4.1).

21. Regarding claim 17, the KASUMI Specification discloses performing the FL function then the FO function, and XORing the output with the lower half of the input or stored result when the round is odd; and performing the FO function then the FL function, and XORing the output with the lower half of the input or stored result when the round is even; and delivering as the partial result the output of the XORing step concatenated with the upper half of the input or stored result (see paragraphs 3.2 and 4.1).

CLAIM REJECTIONS - 35 U.S.C. 103(a)

22. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

23. Claims 5-7 are rejected under the KASUMI Specification, as established above, in view of admitted prior art. The preparers of the KASUMI Specification, the 3GPP Task Force (see page 3), did not state the application of the KASUMI cipher. However, Applicants admit that the 3GPP intended for the KASUMI cipher to be used in an access point (base station), an access terminal (mobile station), and operable in a W-CDMA system (see paragraphs 1003, 1004, 1006, and 1007). In light of the intended use of the KASUMI algorithm, it would have been obvious to use it operable in a W-CDMA system in an access terminal and access point.

CONCLUSION

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel M. Ungar whose telephone number is 571.272.7960. The examiner can normally be reached on 8:30 - 6:00 Monday - Thursday, Alt. Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571.272.3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Art Unit 2132

DMU

Daniel M. Ungar

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100